ADOKit:
Azure DevOps Services Attack Toolkit

Brett Hawkins (@h4wkst3r)

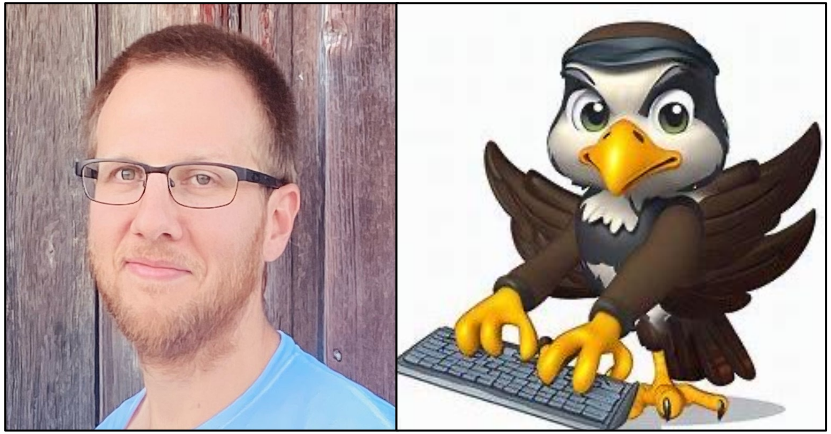
Adversary Services, IBM X-Force Red

Tool:

https://github.com/xforcered/ADOKit

Who am I?

https://h4wkst3r.github.io



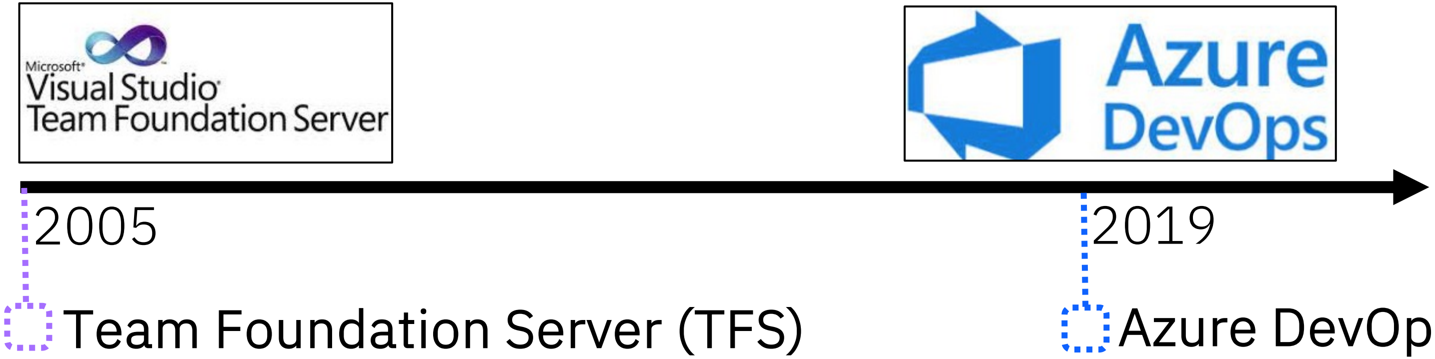
Current Role
Capability Lead,
Adversary Services
IBM X-Force Red

Open-Source Tool Author
SharPersist,
InvisibilityCloak,
SCMKit, ADOKit

Conference Speaker
Black Hat,
DerbyCon, Wild
West Hackin' Fest,
BSides, Hackers
Teaching Hackers

Background

History



2005

2019

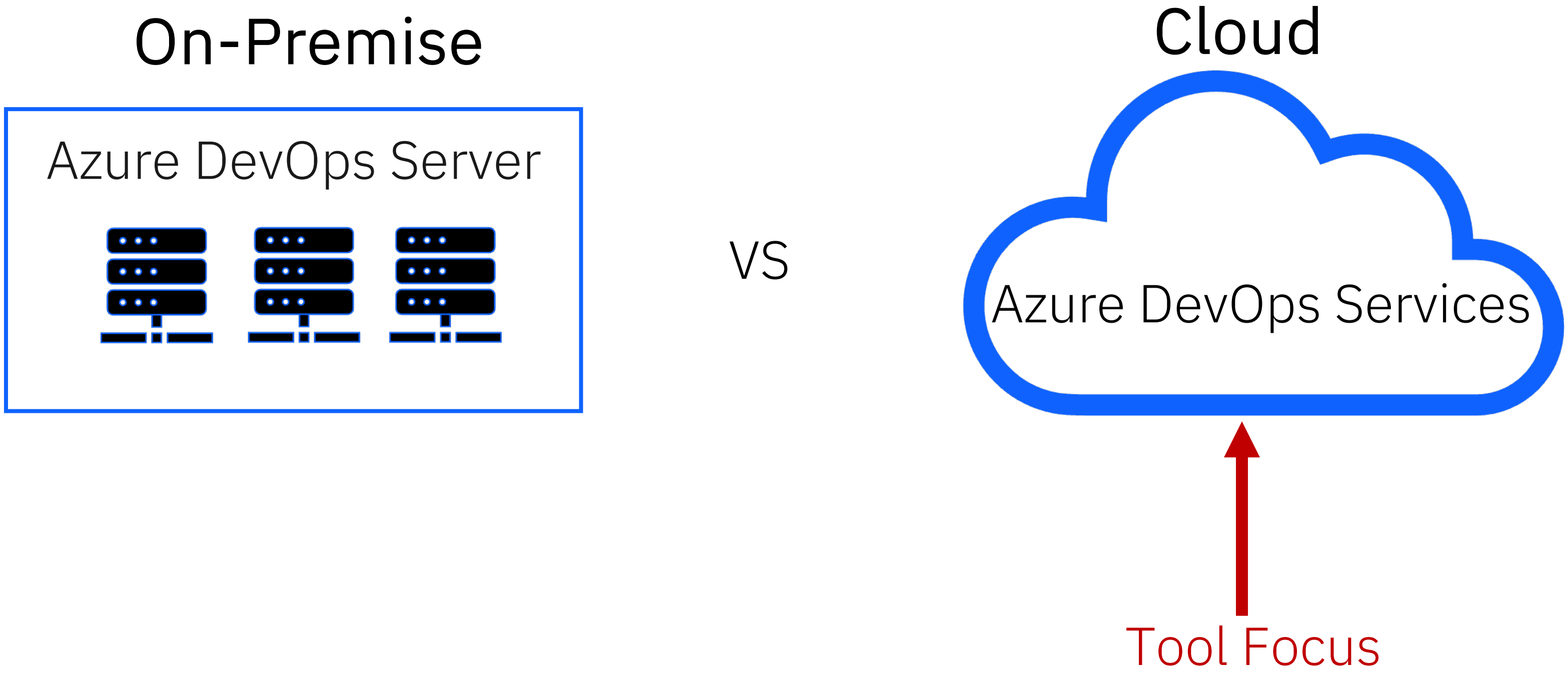
Team Foundation Server (TFS)

- TFS Server
- Visual Studio Team Services (VSTS)

Azure DevOps (ADO)

- Azure DevOps Server
- Azure DevOps Services

Azure DevOps Server vs Azure DevOps Services



On-Premise

Azure DevOps Server

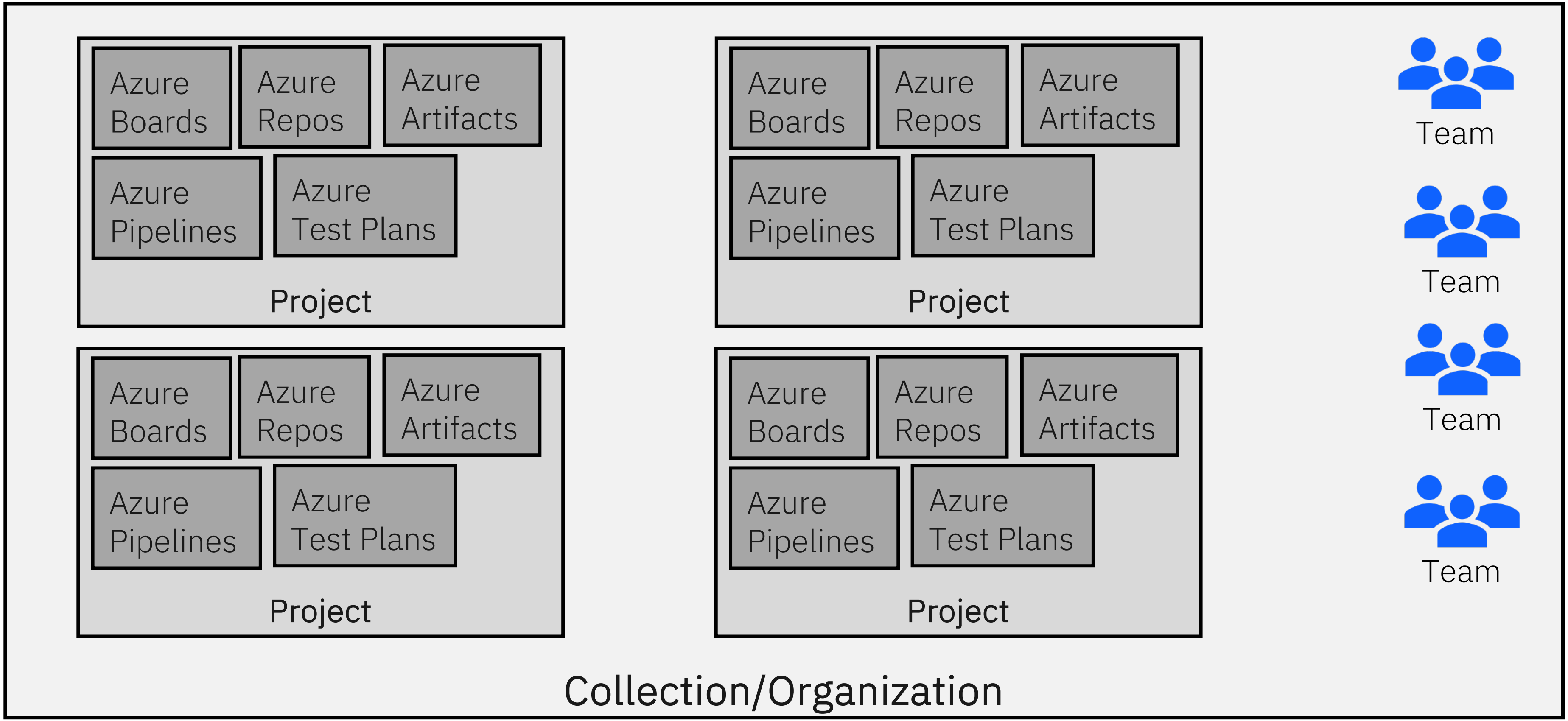
VS

Cloud

Azure DevOps Services

Tool Focus

Common Terminology



Azure Boards

Azure Repos

Azure Artifacts

Azure Pipelines

Azure Test Plans

Project

Azure Boards

Azure Repos

Azure Artifacts

Azure Pipelines

Azure Test Plans

Project

Team

Team

Azure Boards

Azure Repos

Azure Artifacts

Azure Pipelines

Azure Test Plans

Project

Azure Boards

Azure Repos

Azure Artifacts

Azure Pipelines

Azure Test Plans

Project

Team

Team

Collection/Organization

Access and Authorization

Web Interface

Access at https://dev.azure.com/{yourOrganization}

REST API

Programmatic access via OAuth 2.0 or personal access tokens

REST API

Different scopes can be applied for below components

Agent Pools	Analytics	Audit Log	Build
Code	Entitlements	Extensions	Graph & Identity
Load Test	Machine Group	Marketplace	Notifications
Packaging	Project and Team	Release	Security
Service Connections	Settings	Symbols	Task Groups
Team Dashboard	Test Management	Tokens	User Profile
Variable Groups	Wiki	Work Items	

Project Security Groups

Project Administrators

Build Administrators

Project Valid Users

Release Administrators

Contributors

Readers

Organization/Collection Security Groups

Project Collection Administrators

Project Collection Build Administrators

Project Collection Build Service Accounts

Project Collection Service Accounts

Project Collection Proxy Service Accounts

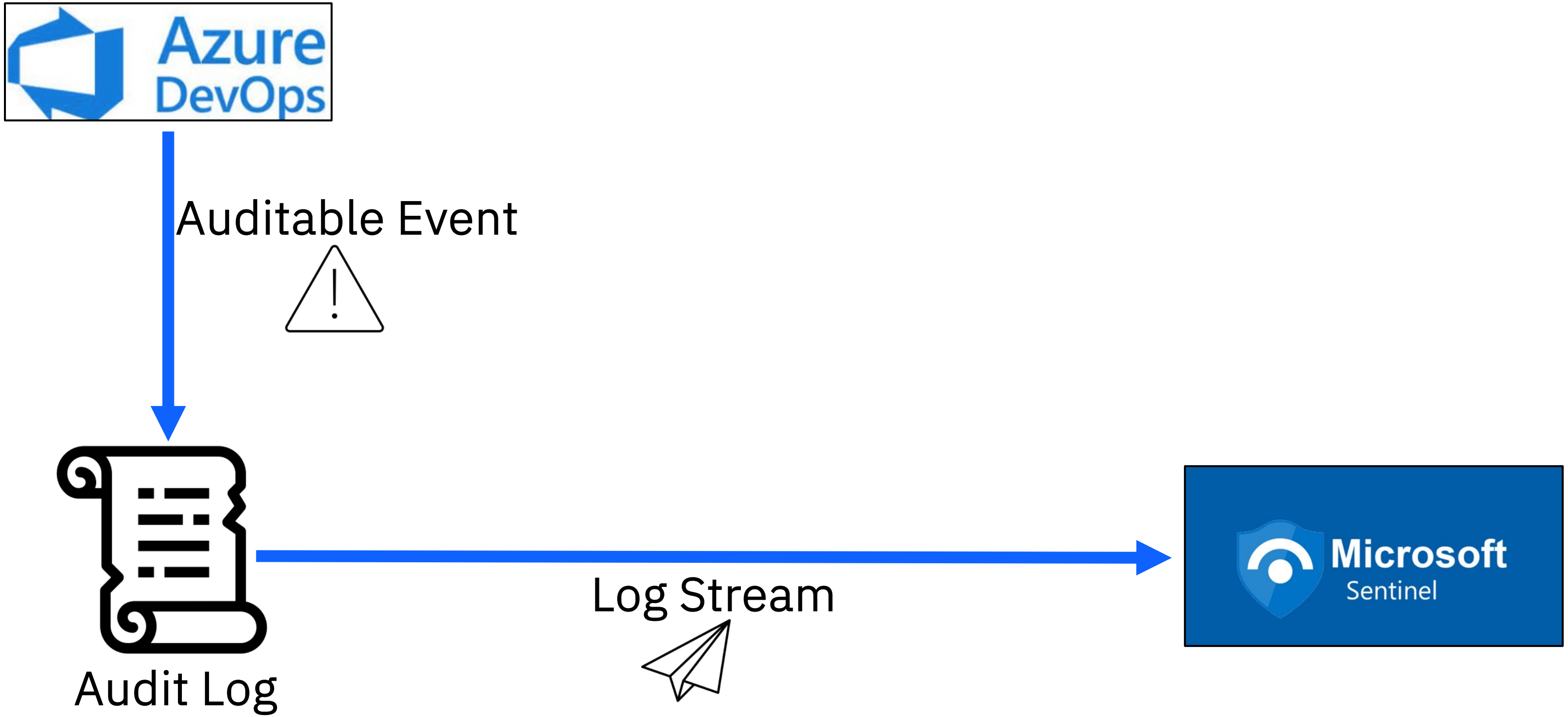
Project Collection Test Service Accounts

Project Collection Valid Users

Project-Scoped Users

Security Service Groups

Logging



Auditable Event

Log Stream

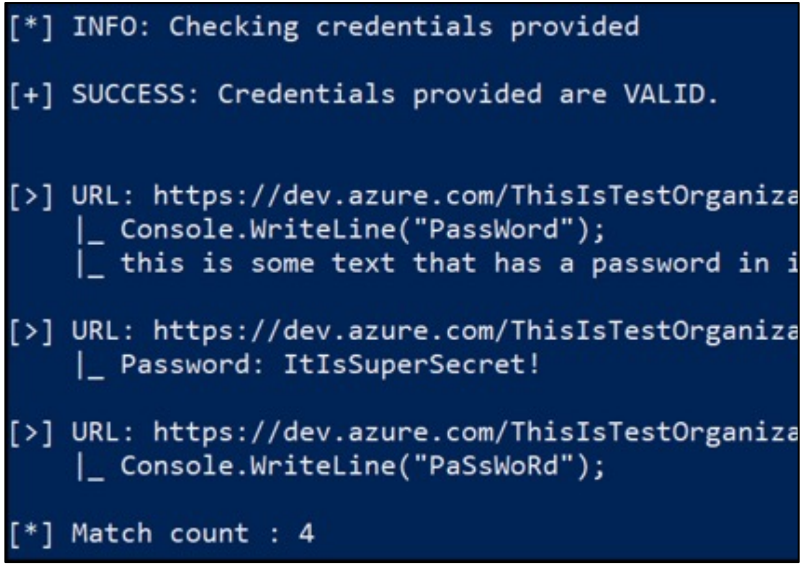
Audit Log

AzureDevOpsAuditing schema

ADOKit

Background

https://github.com/xforcered/ADOKit



```
[*] INFO: Checking credentials provided

[+] SUCCESS: Credentials provided are VALID.


[>] URL: https://dev.azure.com/ThisIsTestOrganiza
    |_ Console.WriteLine("PassWord");
    |_ this is some text that has a password in i

[>] URL: https://dev.azure.com/ThisIsTestOrganiza
    |_ Password: ItIsSuperSecret!

[>] URL: https://dev.azure.com/ThisIsTestOrganiza
    |_ Console.WriteLine("PaSsWoRd");

[*] Match count : 4
```

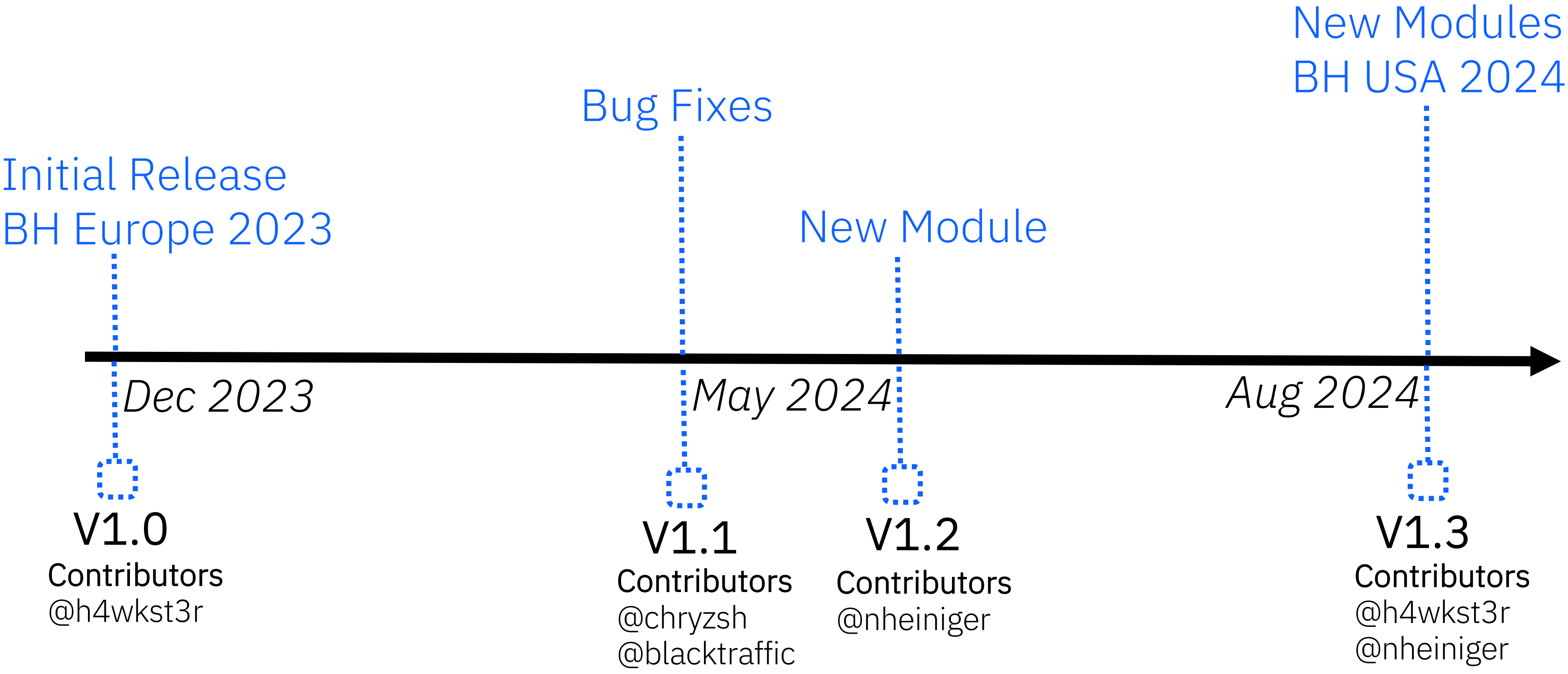
REST API Abuse
Conduct actions programmatically

43 Modules
Recon, Privilege Escalation, Persistence

Authentication
Supports PAT, Access Token or Cookie

Open-Source
Available to community

History



Initial Release
BH Europe 2023

Bug Fixes

New Module

New Modules
BH USA 2024

Dec 2023

May 2024

Aug 2024

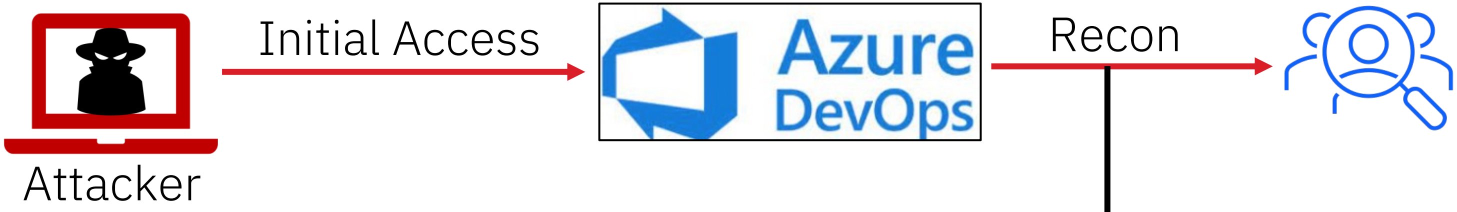
V1.0
Contributors
@h4wkst3r

V1.1
Contributors
@chryzsh
@blacktraffic

V1.2
Contributors
@nheiniger

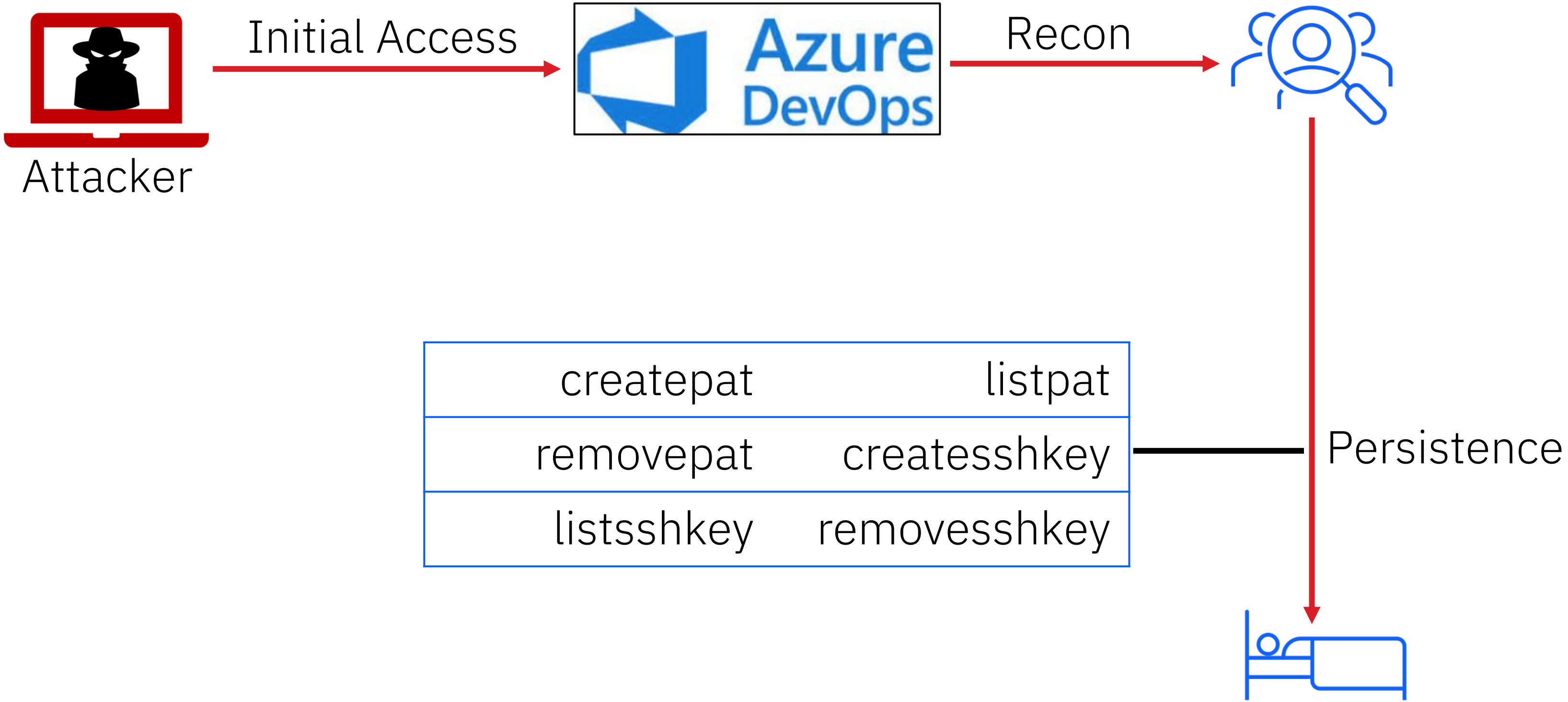
V1.3
Contributors
@h4wkst3r
@nheiniger

Recon Modules



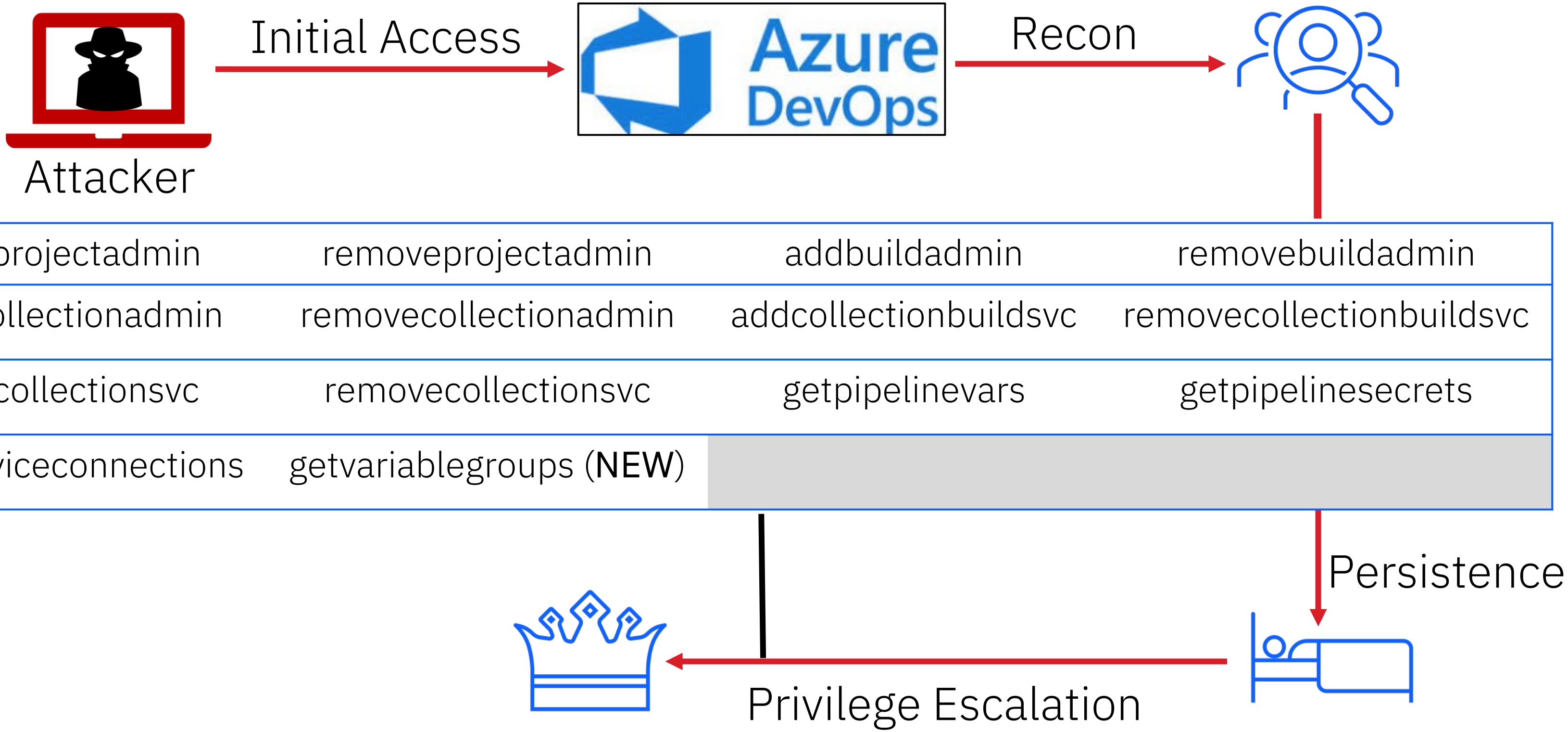
check	whoami	listuser	searchuser
getgroupmembers	getpermissions	listrepo	searchrepo
listgroup	searchgroup	listproject	searchproject
searchcode	searchfile	creds(**NEW**)	getbuildlogs(**NEW**)
listbuildlogs (**NEW**)	searchbuildlogs (**NEW**)	listteam(**NEW**)	searchteam(**NEW**)
getteammembers(**NEW**)			

Persistence Modules



createpat	listpat
removepat	createsshkey
listsshkey	removesshkey

Privilege Escalation Modules



Attacker

Initial Access

Azure DevOps

Recon

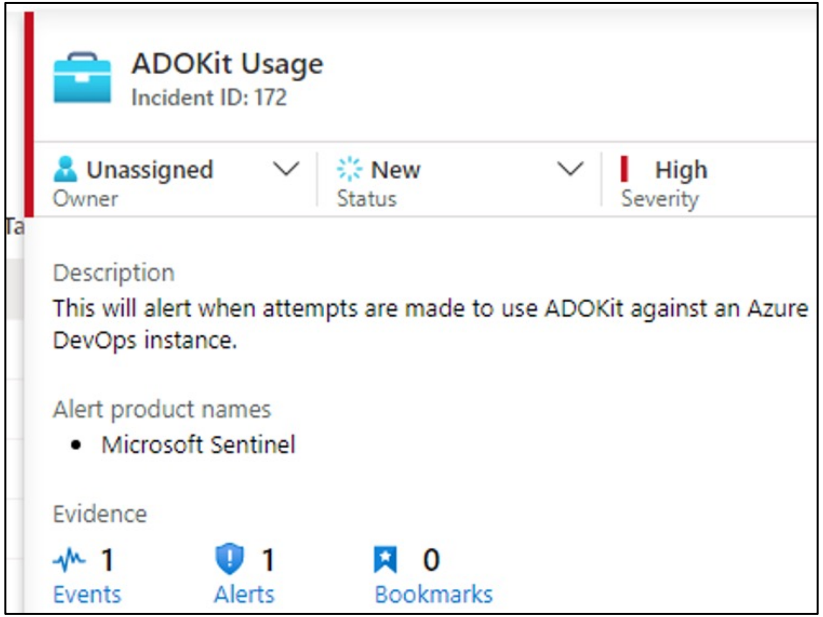
addprojectadmin	removeprojectadmin	addbuildadmin	removebuildadmin
addcollectionadmin	removecollectionadmin	addcollectionbuildsvc	removecollectionbuildsvc
addcollectionsvc	removecollectionsvc	getpipelinevars	getpipelinesecrets
getserviceconnections	getvariablegroups (**NEW**)		

Persistence

Privilege Escalation

Defensive Considerations

ADOKit



ADOKit Usage
Incident ID: 172

Description
This will alert when attempts are made to use ADOKit against an Azure DevOps instance.

Alert product names
- Microsoft Sentinel

Evidence

YARA Rule
C# Project GUID

Snort Rule
Hardcoded user agent string

Sentinel Rules
Any auditable event with ADOKit

Persistence IOC's
PAT and SSH key names prepended with "ADOKit-"

Azure DevOps Services

1 Microsoft Best Practices Guide

2 Integrate proactive secret scanning solution

3 Implement Sentinel rule improvements for ADO

Questions?

Twitter:
@h4wkst3r

Personal Website:
https://h4wkst3r.github.io

Whitepaper:
https://www.ibm.com/downloads/cas/5JKAPVYD

Tool:
https://github.com/xforcered/ADOKit

Thank you

IBM